THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

Rosa E. Rivera Marrero, on behalf of herself and all others similarly situated, Plaintiff, vs. BANCO POPULAR DE PUERTO RICO, a Puerto Rico-based for profit bank, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff, Rosa E. Rivera Marrero ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Banco Popular de Puerto Rico ("Defendant"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information that Defendant's unidentified "vendor" stored on and/or shared using another vendor's "legacy" file sharing platform, including, without limitation, names, addresses, accounts, and/or Social Security numbers (collectively, "personally identifiable information" or "PII").[1]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or

2. According to its website, Defendant "has developed into a large Corporation that offers a great variety of financial products and services, with a presence in the United States, the Caribbean and Latin America."[2]

3. Defendant's customers entrust Defendant with an extensive amount of their PII. Defendant retains this information on computer hardware—even after the customer relationship ends. Its policy and promise to its customers includes "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[3]

4. On or before June 25, 2021, Defendant's unidentified "vendor" informed Defendant that this vendor has experienced a data breach involving Defendant's files (the "Data Breach") and that the Data Breach has occurred via the exploitation of a vulnerability in Accellion FTA ("Accellion FTA"), a legacy software product developed by Accellion, Inc.

5. On or before June 25, 2021, Defendant learned that, during the Data Breach, the unauthorized actor removed one or more documents that contained the PII of Plaintiff and Class Members, including, but not limited to, names, addresses, accounts, and/or Social Security numbers.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals, including the duty to protect and safeguard their PII.

---

valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] *See* https://www.popular.com/en/about-popular/

[3] *See* https://www.popular.com/en/privacy/ (last visited Mar. 7, 2022).

7. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiff and Class Members.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take

available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Rosa E. Rivera Marrero is a citizen of Puerto Rico residing in Toa Alta.

13. Defendant Banco Popular de Puerto Rico is a Puerto Rico-based for profit bank, headquartered at Popular Center Building Suite 913, 209 Munoz Rivera Avenue, San Juan, PR 00918.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

15. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a State different from Defendant to establish minimal diversity.

17. The District of Puerto Rico has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Puerto Rico and this District through its headquarters, offices, parents, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

19. Defendant provided Plaintiff's and Class Members PII to an unidentified "vendor," which used Accellion FTA to store and/or share some of Plaintiff's and Class Members most sensitive and confidential information, including names, addresses, accounts, and/or Social Security numbers, and other personal identifiable information. Notably, much of the information is static, does not change, and can be used to commit myriad financial crimes.

20. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and that Defendant live up to its promises to protect and safeguard their PII.

21. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

22. On or around June 25, 2021, Defendant sent Plaintiff and Class Members a letter information them of the Data Breach. Defendant also provided the Attorney General of Montana

a "sample" notice letter, which stated as follows:

> ***What Happened?***
>
> At **[Banco Popular de Puerto Rico/Popular Bank]** ("Popular"),our customers are out priority, and the security of your information is extremely important to us. We write to inform you that a vendor of Popular has informed us that it was a victim of a cybersecurity breach that included Popular files. Our review has indicated that these files included certain of your personal information. The breach involved the compromise of software owned by Accellion, Inc. that our vendor had used for secure file transfer for its customers, including Popular.
>
> Upon learning of the incident, the vendor immediately launched an investigation, and it also ceased using the impacted software. As a result of this investigation, it was recently determined that certain of the files compromised in the incident included personal information of our customers. Based upon our review, we have determined that this personal information include your **[name, address, account and/or Social Security number]**. This notice explains the complimentary services we have arranged for you, and other steps you may take in response.
>
> We want you to know that we take this topic very seriously and regret that this incident occurred. We are not aware of fraudulent activity in connection with this incident to date.
>
> **Free credit monitoring service:**
>
> As a precaution, we have arranged for you, at your option, to enroll in complimentary, two-year credit monitoring service….[4]

23. Defendant admitted in the notice letter to Plaintiff and the "sample" notice of the Data Breach that an unauthorized party accessed one or more documents that contained sensitive information about Defendant's current and former customers, including names, addresses, accounts, and/or Social Security numbers.

[4] *See* Ex. 1. (sample letter filed with Attorney General of Montana), available at https://media.dojmt.gov/wp-content/uploads/a-notif-42.pdf (last visited Mar. 7, 2022).

24. In response to the Data Breach, Defendant claims that it "ceased using the impacted software."[5] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

25. On May 18, 2021, Accellion announced that 75% of its customers impacted by the exploitation of the vulnerability in Accellion FTA had migrated to another Accellion product known as "Kiteworks."[6] Accellion emphasized that Accellion FTA was a "legacy" product and that Kiteworks was "superior" to FTA. Accellion further asserted that Kiteworks, unlike Accellion FTA, was a "modern, secure" platform for protecting third-party communications.

26. Given the "legacy" status of Accellion FTA and the superiority of Kiteworks in protecting third-party communications, Defendant should have migrated to Kiteworks or another superior solution before the Data Breach occurred.

27. Instead, Defendant continued to use Accellion FTA to share and/or store the PII of Class Members, notwithstanding its "legacy" status and the availability of a "superior" alternative that would have better protected Plaintiff's and Class Members' PII.

28. Defendant's continued use of Accellion FTA, despite the availability of a superior and more secure alternative, resulted in criminals exfiltrating the Social Security numbers and other PII of Plaintiff and Class Members.

29. Plaintiff's and Class Members' unencrypted information may end up for sale on the

[5] Ex. 2.

[6] *See* https://www.accellion.com/company/press-releases/accellion-fta-customers-migrate-to-kiteworks-to-protect-their-most-sensitive-data/ (last visited Mar. 7, 2022).

dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

31. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

32. As a condition of providing services to its customers, Defendant requires that its customers entrust Defendant with highly confidential PII.

33. At all times relevant to this Complaint, Plaintiff's and Class Members were customers of Defendant (or persons who became customers of Defendant through acquisition of their mortgages by Defendant) who entrusted their highly confidential PII (including Social Security numbers) to Defendant and later learned that their PII was compromised in the Data Breach.

34. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

35. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

36. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former customers.

37. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is bewildering given the repeated warnings and alerts about the need to protect and secure sensitive data.

38. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members.

39. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

40. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

41. The PII of individuals remains of high value to criminals, as evidenced by the prices

[7] 17 C.F.R. § 248.201 (2013).

[8] *Id.*

they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, one source reports that personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

42. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

43. What is more, it is no easy task to change or cancel a stolen Social Security number.

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Mar. 7, 2022).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Mar. 7, 2022).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Mar. 7, 2022).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 7, 2022).

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

44. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

46. This data demands a much higher price on the black market. According to Martin Walter, senior director at cybersecurity firm RedSeal, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

47. Among other forms of fraud, identity thieves may obtain driver's licenses,

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Mar. 7, 2022).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 7, 2022).

government benefits, medical services, and housing or even give false information to police.

48. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

49. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

50. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

51. Plaintiff and Class Members now face years of constant monitoring of their financial and personal records and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, including individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed Mar. 7, 2022).

of the unencrypted data.

53. To date, Defendant has offered Plaintiff and Class Members only two years of credit monitoring through a single provider, Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they will face for years to come, particularly in light of the nature of the PII disclosed here.

54. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendant Violated the Gramm-Leach-Bliley Act

55. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

56. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

57. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

58. The GLBA Privacy Rule became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information,

Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

59. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

60. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

61. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Accellion FTA.

62. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on Accellion FTA and would do so after

the customer relationship ended.

63. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

64. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

65. Defendant failed to adequately (a) oversee Accellion and Accellion FTA and (b) require Accellion by contract to protect the security and confidentiality of customer information.

66. As of January 4, 2019, Defendant's "Policies and Procedures" for "Compliance" recognized that the GLBA "prohibits financial institutions from sharing the non-public personal information of consumers with non-affiliated third parties except in certain circumstances."

67. As of January 4, 2019, Defendant further recognized the GLBA required it to (a)

"[p]rovide an opt-out notice prior to sharing non-public personal information with non-affiliated third parties" and (b) "[p]rovide customers with a 'reasonable opportunity' to opt out before disclosing non-public personal information about them to non-affiliated third parties."

68. As of January 4, 2019, Defendant admitted that it had not provided Plaintiff or Class Members an opt-opt notice, stating it "does not currently share non-public personal information with non-affiliated third parties; therefore, it is not required to and does not provide an opt-out notice."

69. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members using Accellion FTA without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

70. Defendant has not informed Plaintiff and Class Members of the reason Defendant shared the PII with the unidentified "vendor;" if this was done to share the PII with a non-affiliated third party, Defendant would be further in breach of the GLBA and its own policy and procedures in failing to provide Plaintiff and Class Members an opt-out notice and a reasonable opportunity to opt out of such disclosure.

Plaintiff's Experience

71. Approximately 30 years ago , Plaintiff opened up checking and saving accounts from Defendant. In connection with those , Plaintiff provided financial and other highly sensitive information to Defendant, including her Social Security Number.

72. On or around June 25, 2021, Plaintiff learned of the Data Breach via the *letter* that Defendant sent to Plaintiff on or around that date.

73. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her financial accounts. This time has been lost forever and cannot be recaptured.

74. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

75. Plaintiff stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

76. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

77. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

78. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

79. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

80. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of

Civil Procedure.

81. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed during the security incident referenced in the notice letter Defendant sent to Plaintiff and others on or around June 25, 2021 (the "Nationwide Class").

82. Excluded from the Classes and Subclasses are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

83. Plaintiff reserves the right to modify or amend the definition of the proposed classes and subclasses before the Court determines whether certification is appropriate.

84. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable.

85. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class and Subclasses exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for

non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, statutory, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

86. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

87. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards

of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

88. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

89. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

90. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

91. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

92. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

93. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members and may continue to act unlawfully as set forth in this Complaint.

94. Further, Defendant has acted or refused to act on grounds generally applicable to the and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

95. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Plaintiff and Class Members are entitled to actual, consequential, statutory, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

96. Plaintiff and the Nationwide Class re-allege and incorporate by reference

paragraphs 1 to 96 as if fully set forth herein.

97. As a condition of being customers of Defendant, Defendant's current and former customers were obligated to provide Defendant with certain PII, including their names, addresses, and Social Security numbers.

98. Plaintiff and the Nationwide Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

99. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

100. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

101. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

102. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

103. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

104. Defendant's duty to use reasonable security measures arose as a result of the special

relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

107. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

108. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

109. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

110. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

111. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

112. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

113. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

114. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

115. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

117. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

118. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

119. There is a close causal connection between Defendant's failure to implement

security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

120. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

121. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

122. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

123. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

124. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on

Accellion FTA, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on Accellion FTA and would do so after the customer relationship ended, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to adequately (i) oversee its Accellion and Accellion FTA and (ii) require Accellion by contract to protect the security and confidentiality of customer information, and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII with one or more non-affiliated third parties.

125. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence *per se*.

126. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act and the GLBA were intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

128. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

129. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

130. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

132. Plaintiff and the Nationwide Class re-allege and incorporate by reference paragraphs 1 to 96 as if fully set forth herein.

133. When Plaintiff and the Nationwide Class provided their PII to Defendant in exchange for Defendant's financial services and products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties after a meeting of the minds—Defendant agreed to take reasonable steps to protect the PII of Plaintiff and the Nationwide Class.

134. Defendant solicited and invited Plaintiff and the Nationwide Class to provide their PII as part of Defendant's regular business practices and as essential to the financial services and products offered. Plaintiff and the Nationwide Class accepted Defendant's offers by providing their PII to Defendant in connection with the purchase of financial services and products from Defendant.

135. Defendant agreed to protect and safeguard the PII of Plaintiff and the Nationwide Class and prevent it from being disclosed or accessed by unauthorized third parties.

136. Defendant required Plaintiff and the Nationwide Class to provide their personal information, including names, addresses, Social Security numbers, and other personal information, as a condition of being customers of Defendant. Defendant may have also required Plaintiff and the Nationwide Class to provide their dates of birth and financial account information as a condition of being customers of Defendant.

137. As a condition of being customers of Defendant, Plaintiff and the Nationwide Class provided their personal and financial information. In so doing, Plaintiff and the Nationwide Class

entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information and to keep such information secure and confidential.

138. Plaintiff and the Nationwide Class value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

139. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

140. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their personal and financial information.

141. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

142. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

143. Plaintiff and the Nationwide Class re-allege and incorporate by reference paragraphs 1 to 96 as if fully set forth herein.

144. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

145. Defendant owed a duty to its current and former customers, including Plaintiff and the Nationwide Class, to keep their PII contained as a part thereof, confidential.

146. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Nationwide Class.

147. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII.

148. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

149. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is of no legitimate concern to the public.

150. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant as part of the current and former customers' relationship with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the

Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

151. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

152. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

153. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

154. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

155. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

156. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

157. Plaintiff and the Nationwide Class re-allege and incorporate by reference paragraphs 1 to 96 as if fully set forth herein.

158. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII that Plaintiff and the Nationwide Class provided to Defendant.

159. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

160. Plaintiff and the Nationwide Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

161. Plaintiff and the Nationwide Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

162. Defendant voluntarily received in confidence the PII of Plaintiff and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

163. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Nationwide Class was disclosed and misappropriated to unauthorized

third parties beyond Plaintiff's and the Nationwide Class's confidence, and without their express permission.

164. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

165. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Nationwide Class's PII as well as the resulting damages.

166. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Nationwide Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII.

167. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on

credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

168. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

169. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

170. Plaintiff and the Nationwide Class re-allege and incorporate by reference paragraphs 1 to 96 as if fully set forth herein.

171. Plaintiff and the Nationwide Class conferred a monetary benefit on Defendant in the form of monies or fees paid for services from Defendant. Defendant had knowledge of this benefit when it accepted the money from Plaintiff and the Nationwide Class.

172. The monies or fees paid by Plaintiff and the Nationwide Class were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and the Nationwide Class.

173. Defendant failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiff and the Nationwide Class, instead storing and/or sharing the PII of Plaintiff and the Nationwide Class using the outdated and vulnerable "legacy" Accellion FTA file transfer platform, which resulted in Plaintiff and the Nationwide Class overpaying Defendant for the services they purchased.

174. Defendant failed to disclose to Plaintiff and the Nationwide Class that Accellion FTA was inadequate to safeguard the PII of Plaintiff and the Nationwide Class against theft.

175. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Nationwide Class because Defendant failed to provide adequate safeguards and security measures to protect the PII of Plaintiff and the Nationwide Class, who paid for such measures but did not receive them.

176. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and the Nationwide Class.

177. Defendant's enrichment at the expense of Plaintiff and the Nationwide Class is and was unjust.

178. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Nationwide Class are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court enter an Order:

A. certifying the Nationwide Class and appointing Plaintiff and her Counsel to represent the Class;

B. enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. providing injunctive or other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption and other means, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

xvii. requiring Defendant to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to PII and to promptly migrate to superior or more secure alternatives;

D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment and post-judgment interest on all amounts awarded; and,

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: May 12, 2022

Respectfully Submitted,

f/ Jorge R. Quintana-Lajara

Lcdo. Jorge R. Quintana Lajara

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

* Denotes Applications for Admission pending or to be filed

QUINTANA & SUÁREZ, L.L.C.
400 Calle Calaf
PMB #165
San Juan, Puerto Rico 00918-1314
Tel. 787-761-1067
787-761-1310
787-309-7531
Fax 787-330-0015
Email: jorgequintanalajara@gmail.com

f/ Jorge R. Quintana-Lajara

Lcdo. Jorge R. Quintana Lajara
RUA 13590

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on May 12, 2022, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

f/ Jorge R. Quintana-Lajara

_____

Lcdo. Jorge R. Quintana Lajara